IN THE CLAIMS:

Please cancel claim1 as presented in the underlying International Application No. PCT/EP00/06510 and cancel revised claims 1-2 annexed to the International Preliminary Examination Report, and add new claims 3-6 as follows:

--3. (new) A method for establishing a common key for a group of at least three subscribers, the method comprising:

generating by each subscriber Ti of the at least three subscribers a respective message Ni = (g^{zi} mod p) from a publicly known element g of large order of a publicly known mathematical group G and a respective random number zi and sending the respective message from the respective subscriber to all other subscribers Tj of the at least three subscribers, each respective random number zi being selected or generated by the respective subscriber Ti;

generating by each subscriber Ti a transmission key k^{ij} from the messages Nj received from the other subscribers Tj, $j \neq i$, and the respective random number zi according to k^{ij}: = Nj^{zi} = $(g^{zj})^{zi}$;

sending by each subscriber Ti the respective random number zi in encrypted form to all other subscribers Tj by generating the message Mij according to Mij := $E(k^{ij}, zi)$, $E(k^{ij}, zi)$ being a symmetrical encryption algorithm in which the data record zi is encrypted with the transmission key k^{ij}; and

determining a common key k by each subscriber Ti using the respective random number zi and the random numbers zj, $j \neq i$, received from the other subscribers according to

$$k: = f(z1, ..., zn),$$

f being a symmetrical function which is invariant under a permutation of its arguments.

4. (new) The method as recited in claim 3 wherein the transmission key k^{ij} is known to subscriber Tj according to $k^{ij} = k^{ji}$.

5. (new) A method for establishing a common key for a group of at least three subscribers, the method comprising:

generating by each subscriber a respective message Ni = (g^{zi} mod p) from a publicly

known element g of large order of a publicly known mathematical group G and a respective random number zi and sending the respective message by each subscriber except a predetermined first subscriber T1 of the at least three subscribers to the first subscriber T1, each respective random number zi being selected or generated by the respective subscriber Ti;

encrypting by the first subscriber T1 the received messages Nj of the other subscribers Tj, $j \neq 1$, with the random number z1 to form a respective transmission key k^{1j} for each subscriber Tj;

sending by the first subscriber T1 the random number z1 to all other subscribers Tj in encrypted form by generating a message M1j according to $M1j := E(k^{1j}, z1)$, $E(k^{1j}, z1)$ being a symmetrical encryption algorithm in which the random number z1 is encrypted with the transmission key k^{1j}; and

determining a common key k by each subscriber Ti using the values Ni and Nj, $j \neq i$, and the random number z1 sent by the first subscriber T1 in encrypted form using

$$k: = h\,(z1, g^{z2}, ..., g^{zn}),$$

h (x1, x2, ..., xn) being a function which is symmetrical in the arguments x2, ..., xn.

6. (new) The method as recited in claim 5 wherein the key is known to subscriber Tj according to $k^{1j} = k^{j1}$.--.

IN THE ABSTRACT:

Please replace the abstract of record with the new abstract submitted herewith as a separate sheet.

REMARKS

New Fig. 1 is submitted herewith for the Examiner's consideration. The application has been amended to place the application in proper format and correct errors. It is respectfully submitted that the claims have not been narrowed. It is respectfully submitted that no new matter has been added.